Cryptology ePrint Archive: Report 2013/110

Full Characterization of Functions that Imply Fair Coin Tossing and Ramifications to Fairness

Gilad Asharov and Yehuda Lindell and Tal Rabin

Abstract: It is well known that it is impossible for two parties to toss a coin fairly (Cleve, STOC 1986). This result implies that it is impossible to securely compute with fairness any function that can be used to toss a coin fairly. In this paper, we focus on the class of deterministic Boolean functions with finite domain, and we ask for which functions in this class is it possible to information-theoretically toss an unbiased coin, given a protocol for securely computing the function with fairness. We provide a \emph{complete characterization} of the functions in this class that imply and do not imply fair coin tossing. This characterization extends our knowledge of which functions cannot be securely computed with fairness. In addition, it provides a focus as to which functions may potentially be securely computed with fairness, since a function that cannot be used to fairly toss a coin is not ruled out by the impossibility result of Cleve (which is the \emph{only} known impossibility result for fairness). In addition to the above, we draw corollaries to the feasibility of achieving fairness in two possible fail-stop models.

Category / Keywords: cryptographic protocols / Fairness, coin tossing, secure computation, malicious and fail-stop adversaries

Publication Info: An extended abstract of this work appeared at TCC 2013. This is the full version.

Date: received 24 Feb 2013

Contact author: asharog at cs biu ac il

Available formats: PDF | BibTeX Citation

Version: 20130227:175557 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]